IN THE CLAIMS

There are no amendments to the claims.

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Previously Presented) A computer-implemented system for protecting a network, comprising:

a vulnerability detection system (VDS) for gathering information about the network to determine vulnerabilities of a plurality of hosts on the network; and

an intrusion detection system (IDS) for examining network traffic responsive to the vulnerabilities of a host from the plurality of hosts as determined by the VDS to detect traffic indicative of malicious activity.

6. (Previously Presented) The system of claim 5, wherein the VDS is adapted to gather information about the network by sending data to the plurality of hosts and receiving responsive data from the plurality of hosts.

7. (Previously Presented) The system of claim 5, wherein the VDS is adapted to gather information automatically provided by the plurality of hosts.

8. (Previously Presented) The system of claim 5, further comprising:

a vulnerabilities rules database, in communication with the VDS, for storing rules describing vulnerabilities of the plurality of hosts,

wherein the VDS is adapted to analyze the gathered information with the rules to determine the vulnerabilities of the plurality of hosts.

9. (Previously Presented) The system of claim 8, wherein the VDS is adapted to analyze the gathered information with the rules to identify operating systems on the plurality of hosts and determine the vulnerabilities responsive to the respective operating systems.

10. (Previously Presented) The system of claim 8, wherein the VDS is adapted to analyze the gathered information with the rules to identify open ports on the plurality of hosts and determine the vulnerabilities based on the open ports.

11. (Previously Presented) The system of claim 8, wherein the VDS is adapted to analyze the gathered information with the rules to identify applications executing on the plurality of hosts and determine the vulnerabilities based on the applications.

12. (Original) The system of claim 5, further comprising:

an intrusion rules database, in communication with the IDS, for storing rules describing malicious activity,

wherein the IDS is adapted to analyze the network traffic with the rules to detect network traffic indicative of exploitations of the determined vulnerabilities.

13. (Original) The system of claim 5, wherein the IDS is adapted to detect traffic indicative of exploitations of only the determined vulnerabilities.

14. (Cancelled)

15. (Original) The system of claim 5, wherein the VDS is adapted to update the determined vulnerabilities, and wherein the IDS is adapted to detect traffic indicative of malicious activity in response to the update.

16. (Original) The system of claim 15, wherein the VDS is adapted to update the determined vulnerabilities in response to a change in the network.

17. (Previously Presented) A computer-implemented method for protecting a network, comprising:

gathering information about the network to determine vulnerabilities of a plurality of hosts on the network; and

examining network traffic responsive to the determined vulnerabilities of a host from the plurality of hosts to detect network traffic indicative of malicious activity.

18. (Previously Presented) The method of claim 17, wherein gathering information comprises sending data to plurality of hosts on the network and receiving responsive data from the plurality of hosts.

19. (Previously Presented) The method of claim 17, wherein gathering information comprises receiving data automatically provided by the plurality of hosts on the network.

20. (Previously Presented) The method of claim 17, further comprising:

storing rules to describe vulnerabilities of the plurality of hosts,

wherein determining vulnerabilities includes analyzing the gathered information with the rules.

21. (Previously Presented) The method of claim 20, wherein determining vulnerabilities comprises analyzing the gathered information with the rules to identify operating systems on the plurality of hosts.

22. (Previously Presented) The method of claim 20, wherein determining vulnerabilities comprises analyzing the gathered information with the rules to identify open ports on the plurality of hosts.

23. (Previously Presented) The method of claim 20, wherein determining vulnerabilities comprises comparing the gathered information against the rules to identify applications on the plurality of hosts.

24. (Original) The method of claim 17, further comprising:

storing rules describing malicious activity,

wherein detecting network traffic indicative of malicious activity comprises analyzing the network traffic with the rules to detect traffic indicative of exploitations of the determined vulnerabilities.

25. (Original) The method of claim 17, wherein examining network traffic consists of detecting traffic indicative of exploitations of only the determined vulnerabilities.

26. (Cancelled)

27. (Previously Presented) The method of claim 17, further comprising:

updating the determined vulnerabilities and detecting traffic indicative of malicious activity in response to the update.

28. (Original) The method of claim 27, wherein the updating is responsive to a change in the network.

29. (Previously Presented) A computer program product, comprising:

a computer-readable medium having computer program logic embodied therein for protecting a network, the computer program logic:

gathering information about the network to determine vulnerabilities of a plurality of hosts on the network; and

examining network traffic responsive to the determined vulnerabilities of a host from the plurality of hosts to detect network traffic indicative of malicious activity.

30. (Previously Presented) The computer program product of claim 29, wherein gathering information comprises sending data to plurality of hosts on the network and receiving responsive data from the plurality of hosts.

31. (Previously Presented) The computer program product of claim 29, wherein gathering information comprises receiving data automatically provided by the plurality of hosts on the network.

32. (Previously Presented) The computer program product of claim 29, further comprising:

storing rules to describe vulnerabilities of the plurality of hosts,

wherein determining vulnerabilities includes analyzing the gathered information with the rules.

33. (Previously Presented) The computer program product of claim 32, wherein determining vulnerabilities comprises analyzing the gathered information with the rules to identify operating systems on the plurality of hosts.

34. (Previously Presented) The computer program product of claim 32, wherein determining vulnerabilities comprises analyzing the gathered information with the rules to identify open ports on the plurality of hosts.

35. (Previously Presented) The computer program product of claim 32, wherein determining vulnerabilities comprises comparing the gathered information against the rules to identify applications on the plurality of hosts.

36. (Original) The computer program product of claim 29, further comprising:

storing rules describing malicious activity,

wherein detecting network traffic indicative of malicious activity comprises analyzing the network traffic with the rules to detect traffic indicative of exploitations of the determined vulnerabilities.

37. (Original) The computer program product of claim 29, wherein examining network traffic consists of detecting traffic indicative of exploitations of only the verified vulnerabilities.

38. (Cancelled)

39. (Previously Presented) The computer program product of claim 29, further comprising:

updating the determined vulnerabilities; and

detecting traffic indicative of malicious activity in response to the update.

40. (Previously Presented) The computer program product of claim 39, wherein the updating is responsive to a change in the network.